Information Survivability: Required Shifts in Perspective

Julia H. Allen and Dr. Carol A. Sledge
Software Engineering Institute

Organizations today are part of an interconnected, globally networked environment – one that continuously evolves in ways that cannot be predicted. What effect does this environment have on the survivability of the mission of an organization? To improve survivability, organizations must shift their focus from a more information security-centric perspective to one that includes an information survivability-centric perspective.

The events of recent years and especially of recent months have greatly increased awareness of information and infrastructure security, whether they are media reports of the latest cyber attacks and vulnerabilities or postulations as to the degree of permeability of our critical infrastructures.

While this may spark reactions such as reviews of organizational computer security policies and vulnerability assessments, attention to issues of security, while important [1], cannot ensure the preservation of mission-critical services when systems are penetrated or compromised. Survivability, an emerging discipline, incorporates a new technical and business perspective on security, creating solutions that focus on elements such as the continuity of critical services.

In terms of solution space, security takes a technology centric point of view, with each technology solving a specific set of issues and concerns that are generally separate and distinct from one another. Survivability takes a broader, more enterprise-wide point of view looking at solutions that are more pervasive than point-solution oriented.

Survivability

We define survivability as "the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents" [2]. A survivability approach combines risk management and contingency planning with computer security to protect highly distributed information services and assets in order to sustain mission-critical functions. Survivability expands the view of security from a narrow, technical specialty understood only by security experts to a risk management perspective with participation by the entire organization and stakeholders.

To improve the survivability of the organization's mission, senior management must shift its focus and that of the organization from an information technology (IT)-based, security-centric, technology solution perspective to an enterprise-based, survivability-centric, risk management perspective. Experience in our executive workshop[1] has shown that many do not know how to think about information survivability in a useful way, or understand the role they should play in promoting survivability.

Seven Shifts in Perspective

We have observed seven shifts in perspective or shifts in thinking that we believe are essential to move from an IT-based, security-centric, technology solution point of view to one that is more enterprise wide, based on survivability and builds on risk management (Table 1).

For each of these seven shifts in perspective, we describe some example indicators. The presence or absence of these indicators may give some notion of whether or not the shift is in progress, or if it has actually occurred. We do not claim these indicators are definitive or comprehensive, but merely exemplars. Similarly, we present examples of questions senior management can ask to elicit the current state of the organization.

Asking the right questions is essential for senior management to understand the critical role that survivability plays in fulfilling its mission and objectives, as well as the risks that need to be managed [3]. Creating organizational awareness about survivability is essential for it to be factored into key decisions. This assumes that mission and information survivability are high priorities when weighed against other pressing priorities that vie for senior management's attention.

Shift 1: Central to Global

The first shift in perspective is from systems that are in a centrally networked environment under organizational control with full visibility, to systems that are in a globally networked environment with no bounds, no central control, and limited visibility into the systems. Physically isolated, stand-alone mainframe or corporate environments have evolved into a distributed client server network that are connected to the Internet with peer-to-peer services and networking. It is no longer the case that access is permitted only within the physical facilities that house the network: Remote access is now a given.

This shift in perspective may be indicated by actions taken to regularly evaluate and address key risks to key assets based on global access and often unknown threats from unidentified sources. It may also be indicated by the presence of a network/system architecture where critical assets (including functions/services) are distributed and stored redundantly [4].

Questions to initiate or indicate this shift include the following:

- Is the frequency and scope of the organizational risk evaluation sufficient to evaluate key risks to key assets

Table 1: *Seven Shifts in Perspective*

FROM	TO
Systems are centrally networked, under organizational control.	Systems are globally networked with distributed control.
Systems are bounded with defined geopolitical boundaries.	Systems are unbounded with no geopolitical boundaries.
Clear distinction between insiders and outsiders.	Often cannot distinguish between insiders and outsiders.
Predictable processing load and events.	Unpredictable load and asynchronous events.
Organizational responsibility.	Distributed responsibility.
Security as an overhead expense.	Survivability as an investment; essential to the organization.
Technology, IT-based solutions.	Enterprise-wide, risk management solutions.

and take into account evolving threats?
- Does the continuity plan sufficiently address how to protect the confidentiality, integrity, and availability of critical assets?
- Is the security policy sufficient and effectively enforced for today's globally distributed environment?

Shift 2: Bounded to Unbounded

The second shift in perspective is from systems that have well-defined geographic, political, cultural, and legal or jurisdictional boundaries, to systems characterized by the absence of these boundaries. Centralized administrative control with trustworthy, known, inside users evolves to systems with distributed administrative control without central authority and unknown users. This shift is also indicated by the presence of an active network of administrators with time to stay up-to-date, stay connected, and stay in communication with one another.

Questions to initiate or indicate this shift include the following:
- Do strategic and tactical security decisions derive from an appreciation that networks, when connected to the Internet, have no well-defined geographical, political, and technological boundaries?
- Do system and network administrators have an active contact list of peers for the primary networks interfaced?
- Are administrators up-to-date on the latest threats, attacks, and solutions?
- Are system and network configurations up-to-date with the latest patches?

Shift 3: Insular to Networked

The third shift in perspective is from viewing systems as insular and fortress-like, to viewing systems as being networked and interdependent; the ability to distinguish between insiders and outsiders decreases. Outsider roles go from being well-defined to the realization that an outsider can be a customer, collaborator, partner, contractor, or vendor; outsider access to the network changes based on that role. Do we have layered security architecture (*defense in depth*), understanding that organizational perspective shifts from thinking a firewall will protect the network to the realization that a firewall is just one part of layered security architecture? In-house infrastructure maintenance may shift to the outsourcing of all or part of the infrastructure and may include managed security services (e.g. firewalls, intrusion detection monitoring, incident response, and penetration testing).

This shift may be indicated by the presence of a decision process allowing third-party access, with active management of each type of relationship with the appropriate level of security. Secure means exist for remote access, authentication, and access control; virtual private network technologies may be used. Accounts are retired when partnerships or relationships terminate.

Questions to initiate or indicate this shift include:
- Do we have a layered security architecture?
- Are there decision processes and supporting procedures to permit third-party access and to manage each type of relationship with the appropriate level of security?
- Do we understand and implement appropriate security controls for managed security services provided by outside parties?

"Outsider roles go from being well-defined to the realization that an outsider can be a customer, collaborator, partner, contractor, or vendor; outsider access to the network changes based on that role."

Shift 4: Predictable to Asynchronous

The fourth shift in perspective is from one where processing events happen in predictable, prescribed sequences and patterns with predictable loads, to one where events often occur asynchronously, independent of time sequence with unpredictable loads. The situation becomes one where anything can happen anytime: Work proceeds 24 hours a day, seven days a week, and distributed denial-of-service agents can be installed and launched at any time.

A clear understanding and management of risk where predictability is important indicate evidence of the shift. It may be necessary to take these particular processes offline, to create an *air gap*. The shift is also manifested by diligence to ensure installed attack agents are detected and eliminated.

Questions to initiate or indicate this shift include:
- Are processes and transactions that need to occur in a predictable sequence sufficiently protected from disruption?
- Do administrators regularly scan for the presence of denial-of-service agents?
- Is the integrity baseline maintained and regularly checked for all critical assets?

Shift 5: Single Responsibility to Shared Responsibility

The fifth shift in perspective progresses from single responsibility to shared organizational responsibility to distributed responsibility. This is a shift from having a single point of known responsibility to correct failures, to having shared sometimes unknown responsibility. In other words, going from, "I know who to contact when I have a problem and I can describe the problem" to a situation better described as, "I cannot precisely identify what or where the problem is, and I may not know who to contact if it occurs outside of my organization's administrative control."

The shift is indicated by everyone knowing who to call first inside of the organization, with the responder performing triage on all calls. That responder relies on his/her contact list for assistance and solutions. Those collectively responsible understand their high degree of interdependence and are quick to assist.

Questions to initiate or indicate this shift include:
- Do all authorized users know whom to contact when they detect suspicious, unexpected, or unusual behavior?
- Do the recipients of this information know how to process each request, dealing with highest priority requests first, and know who to contact for further assistance?

Shift 6: Overhead to Essential

The sixth shift in perspective is from viewing security as an overhead activity and expense, to viewing survivability as an investment that is essential to the organization, along with ensuring that there is always a contingency plan. It reflects a change of view. Instead of security being IT's responsibility, with IT and the CIO constantly having to justify their budget for security, survivability is regularly reviewed and discussed in senior-level management meetings and is accept-

ed by all as part of being in business.

Questions to initiate or indicate this shift include:

- Is the term *survivability* an active part of the vocabulary at all organizational levels?
- Is survivability regularly reviewed and discussed in senior-level management meetings?
- Is work to sustain/improve security and survivability a standing budget line item that does not require annual justification?
- Do continuity and disaster recovery plans adequately address security and survivability concerns? Are these plans regularly tested?

Shift 7: Security to Survivability

The seventh shift in perspective is from technologic IT-based solutions to enterprise-wide, risk-management solutions. Instead of viewing security as a narrow, technical specialty accessible only to experts and focusing on the protection of specific components, survivability is embraced as a risk-management perspective that requires involvement of the whole organization and focuses on the survival of the mission rather than a particular component.

Senior managers must change their view that "protecting the network is a matter of listening to the right experts and installing the right technology solutions." Rather, their declared view is that "the survival of the mission depends on the ability of the network to provide continuity of service, albeit degraded, in the presence of attacks, failures, or accidents."

The shift is indicated by the absence of silver-bullet thinking. It is replaced by understanding that this is a long-term, continuous activity required for the success of the organization. In other words, senior management needs to think of survivability and its contribution to the organization the same way that they would think of any critical organizational process or organizational function that they perform (such as meeting profit objectives, growing through acquisition, and raising stockholder share value). Survivability must have the same importance and receive the same level of attention as any of those other key processes.

Questions to initiate or indicate this shift include the following:

- Are security and survivability risks managed as actively as other risks?
- Is it understood (as manifest in our speaking and actions) that the survivability of the infrastructure is essential to the survivability of the organization and mission?
- Are IT staff members involved in executive and management-level decisions on security and survivability and vice versa?

Summary

Given that more and more of today's organizations are part of an interconnected, globally networked community, this shift in thinking is imperative. The survivability of an organization's mission requires that senior management and their organizations shift their thinking from an IT-based, security-centric, technology solution point of view, to one that is more enterprise-wide, based on survivability and that utilizes risk management approaches. As a start, for each of the seven shifts in perspective, think about where your organization is today: Has it already accomplished the shift? Is it in progress? How might this shift be initiated? ◆

References

1. Allen, Julia, Christopher Alberts, Sandi Behrens, Barbara Laswell, and William Wilson. "Improving the Security of Networked Systems." CROSSTALK Oct. 2000.
2. Lipson, Howard, and David Fisher. "Survivability – A New Technical and Business Perspective on Security." Proceedings of the 1999 New Security Paradigms Workshop. Association for Computing Machinery. New York, 1999. Available at <www.cert.org/archive/pdf/busperspec.pdf>.
3. Allen, Julia H. "Ask the Right Questions." Internet Security Alliance. 26 Oct. 2001. Available at <www.isalliance.org/working/practices.phtml>.
4. Linger, Richard C., Robert J. Ellison, Thomas A. Longstaff, and Nancy R. Mead. "The Survivability Imperative: Protecting Critical Systems." CROSSTALK Oct. 2000.

Note

1. "Survivability: A New Executive Perspective" is a course offered by the Software Engineering Institute, Carnegie Mellon University, Pittsburgh.

About the Authors

Julia H. Allen is a senior member of the technical staff of the Software Engineering Institute (SEI). Her work includes the development of security improvement practices for network-based systems. She previously served as SEI acting director and deputy director. Before joining the SEI, she was vice president of Science Applications International Corporation (SAIC), where she was responsible for starting a division that specialized in embedded systems software. She recently published *The CERT Guide to System and Network Security Practices.*

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
Phone: (412) 268-7995
Fax: (412) 268-7966
E-mail: jha@sei.cmu.edu

Carol A. Sledge, Ph.D., is a senior member of the technical staff of the Software Engineering Institute (SEI). Her work includes executive education and the investigation of practices and strategies for survivable enterprise management. Dr. Sledge previously investigated commercial off-the-shelf based and open systems. Before joining the SEI, she managed the acquisition, development, and support of large multiplatform, system-software product lines at a number of corporations. Dr. Sledge has developed and taught a variety of software engineering and computer science courses.

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Room SEI/SP 406
Pittsburgh, PA 15213-3890
Phone: (412) 268-7708
Fax: (412) 268-7966
E-mail: cas@sei.cmu.edu